

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A
Person and Property to Be Searched

1. The person of SAMONE THOMAS (B/F, DOB: XX/XX/1990).
2. THOMAS's Apple iPhone, bearing phone number (414) 779-3186.

ATTACHMENT B
Particular Things to be Seized

1. All records, information, and items related to violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. Section 1320a-7b (Illegal Kickbacks), occurring on or after February 2021, including:

- a. Evidence of communications, photographs, or videos relating to Prenatal Care Coordination client recruitment; care coordinator recruitment; billing; compensation; and/or care coordinator meetings;
- b. Evidence of the performance of care-coordination duties including, but not limited to, communications with clients of Caring Through Love, LLC;
- c. Evidence of communications with individuals for whom Caring Through Love LLC billed for services;
- d. Evidence of communications with care coordinators or owners of care coordinator businesses;
- e. Evidence of compensation or gifts provided by Caring Through Love or Precious Cruse;
- f. Evidence of gifts or items provided to individuals for whom Caring Through Love LLC billed for services
- g. Evidence of travel out of the State of Wisconsin during the period between February 2021 and September 2021;
- h. Evidence of financial transactions related to the provision of care-coordinator services and/or employment with Caring Through Love LLC;
- i. For computers, cellphones, and electronics capable of communication or storage (collectively, “computers”):
 - i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - ii. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - iii. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;

- iv. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- vi. evidence of the times the computer was used;
- vii. passwords, encryption keys, and other access devices that may be necessary to access the computer;
- viii. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- ix. records of or information about Internet Protocol addresses used by the computer;
- x. records of or information about the computer's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- xi. contextual information necessary to understand the evidence described in this attachment;
- xii. lists of contacts and any identifying information.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of SAMONE THOMAS to the fingerprint scanner of the device; (2) hold a device found in front of the face of SAMONE THOMAS and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

Briefly describe the property to be searched
or identify the person by name and addressThe person and cellular phone of
SAMONE THOMAS (DOB: XX/XX/1990),
as more fully described in Attachment A.

Case No.22-1838M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location)

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. Sections 1347 and
1035; 42 U.S.C. Section
1320a-7b


Offense Description

Healthcare Fraud: False Statements Related to Healthcare: Illegal Kickbacks

The application is based on these facts:

See Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



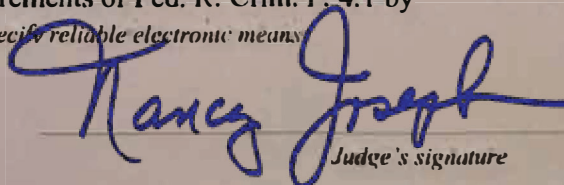
Applicant's signature

FBI SA Jill A. Dnng

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means)

Date: 11/21/2022



Judge's signature

City and state: Milwaukee, Wisconsin

U.S. Magistrate Judge Nancy Joseph

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jill A. Dring, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of a person, and the extraction of evidence from that person as described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since March of 2013. As a Special Agent, I investigate civil and criminal matters related to health care fraud involving violations of the Health Care Fraud Statute, False Claims Act, Anti-Kickback Statute and Stark Law. Prior to investigating health care fraud matters, I investigated criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of identification information, and other computer-based fraud. I have received training in computer technology, computer-based fraud and health care fraud.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that PRECIOUS CRUSE (DOB: 06/07/1993), SAMONE THOMAS (DOB: 02/05/1990), and others known and unknown to the case agents have committed violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. Section 1320a-7b (Illegal Kickbacks).

4. Further, there is probable cause to search the locations described in Attachment A for evidence of these crimes, as described in Attachment B.

PERSON AND PROPERTY TO BE SEARCHED

5. The person of SAMONE THOMAS (DOB: 02/05/1990).

6. THOMAS's Apple iPhone, bearing phone number (414) 779-3186.

PROBABLE CAUSE

7. On 9/28/21, members of the Medicaid Fraud Control & Elder Abuse Unit (MFCEAU), were assigned Department of Justice Investigation case number 2021-07738, involving a credible allegation of fraud referral from Department of Health Services (DHS) Office of the Inspector General (OIG) pertaining to Caring Through Love, a Prenatal Care Coordination (PNCC) agency owned by PRECIOUS CRUSE. A Prenatal Care Coordination (PNCC) agency is an agency that provides services to pregnant women who are at high risk for adverse pregnancy outcomes. PNCC services are reimbursed under Wisconsin Medicaid when provided in accordance with Wisconsin Medicaid's rules and regulations. Covered services related to PNCC services are listed in Wis. Admin. Code § DHS 107.34.

8. Per Wis. Admin. Code § DHS 107.34, PNCC agencies are required to have a Qualified Professional. Prior to services being performed for a Medicaid recipient by a PNCC, and the subsequent reimbursement by Wisconsin Medicaid, an initial assessment and care plan are required. The Qualified Professional reviews and signs the assessment.

9. The PNCC program requires providers to submit accurate and truthful claims for payments. It also requires a provider to only seek reimbursement for the actual amount of time spent assisting a member. And it prohibits providers from seeking reimbursement for non-covered services. Examples of non-covered services include personal comfort items such as radios and television sets. DHS 107.03(6). Additionally, DHS has explained that if a client is in need of something like diapers or wipes, a care coordinator should connect the client with an organization that can provide those items, rather than providing them. The PNCC program prohibits seeking reimbursement for noncovered services by charging for a covered service that was not actually

provided.

10. On 9/28/21, MFCEAU accepted a credible allegation of fraud referral from DHS OIG. The allegations stated that Caring Through Love, LLC (CTL), offered illegal incentives to its members and/or prospective members to enroll in the program. Additionally, there are allegations that CTL, intentionally made false statements or representations of material facts on a claim to obtain payment for services provided without the supervision of a Qualified Professional.

11. According to records kept by DHS in the regular course of its official business, Vivian Mealing, RN, is listed as the Qualified Professional at CTL. Barbara Hayden, an OIG nurse consultant, contacted Vivian Mealing, and during a conversation that occurred on 4/1/21, Mealing informed Hayden that she has yet to perform any services for CTL.

12. DHS launched and completed an investigation prior to sending MFCEAU the credible allegation of fraud. DHS reviewed Facebook posts of Presh Hutchinson that appeared to offer monetary incentives to clients for Mother's Day. As substantiation for the allegation, DHS OIG provided a screenshot or screen capture of the Facebook post made by Presh Hutchinson. A screenshot or screen capture is a digital image that shows the content of a computer or digital display.

13. Case agents reviewed the screenshot provided by DHS OIG. The screenshot in question is a Facebook post from 05/27/2021, posted under the account of Presh Hutchinson. It reads, "Happy Mother's Day To All the Clients Enrolled With Caring Through Love LLC We Appreciate Yall, & I hope Yall Enjoy Your Gifts From Us & Your Day." A photograph and video are attached to the post. In the photo, and screen still from the video, there is \$100 in \$20 bills in a card.

14. Based on my training and experience, I know that Wisconsin Medicaid does not

allow monetary incentives to potential or existing clients, and it is viewed as an illegal incentive, or a kickback. The Wisconsin Medicaid Provider Agreement and Acknowledgement of Terms of Participation (WMPAATP), set forth by Wis. State § 49.045(2)(a)9, and Wis. Admin Code §DHS 105.01, state that a provider, in this case CRUSE and CTL understands and agrees that every time the provider signs and submits a claim, the provider certifies that the provider has not offered, paid, or received any illegal remuneration or any other thing of value in return for referring an individual to a person for the furnishing of any service or item, or for arranging for the furnishing of any service or item for which payment may be made in whole or in part under Medical Assistance in violation of 42 U.S.C. § 1320a-7b, Wis. Stat. § 946.91(3), or any other federal or state anti-kickback statutes. The WMPAATP was signed by CRUSE on 02/04/2021.

15. Case agents reviewed Wisconsin Medicaid records kept by DHS in the regular course of its official business and learned that CRUSE is the current and past owner of CTL. Case agents confirmed that CRUSE was the owner of CTL, at the times of the suspect posts.

16. In February 2022, I joined MECEAU's investigation of CTL.

17. On October 3, 2022, I, along with MECEAU investigator Rory O'Sullivan interviewed Tia Imes, who was a registered client of CTL. CTL business records demonstrated that Samone THOMAS was Tia Imes' care coordinator. CTL billed \$1,056 to Medicaid for PNCC services purportedly provided to Ms. Imes on 10 separate dates. Ms. Imes told investigators that she signed up for services with CTL at a "community baby shower" at which she received diapers, wipes, and a pack 'n play. Ms. Imes said that she was never thereafter contacted by anyone with CTL and received no services. The first day of service billed for Ms. Imes was August 6, 2021. Ms. Imes states that she was in the hospital recovering from the birth of her child that day and did not meet anyone from CTL that day.

18. On October 3, 2022, I, along with MECEAU investigator Rory O'Sullivan, interviewed Tenisha Woulard. Woulard was a client of CTL. CTL billed \$2,112 for services purportedly provided to Ms. Woulard on 22 separate occasions. She indicated during the interview that she received no services and only had one meeting with a representative from CTL. Samone THOMAS was listed as Ms. Woulard's care coordinator.

19. On October 3, 2022, I, along with MECEAU investigator Rory O'Sullivan, interviewed three other women for whom CTL submitted billing claims to Medicaid for PNCC services purportedly provided by THOMAS. Some were billed for services as early as February 2021. All the women indicated that they received no coordination services. Some indicated that they received outfits, diapers, and fireworks. We showed these clients billing records describing meetings and services purportedly provided. Each denied that the meetings occurred or that the services were provided. At least one woman interviewed denied knowing THOMAS.

20. On November 16, 2022, I, along with Rory O'Sullivan and AUSAs Julie Stewart and Kate Biebel, interviewed THOMAS. During the meeting, she produced her cellular phone, an Apple iPhone, and consulted it on several occasions to view photos and videos while responding to our questions. I know the phone number associated with THOMAS's iPhone is (414) 779-3186; I know this because AUSA Stewart called THOMAS on that number, which THOMAS previously provided, on the morning of November 16, 2022 to confirm the meeting. THOMAS stated she forgot and asked AUSA Stewart to text her the address of building where the meeting was to take place. AUSA Stewart sent a text message to that number with the information THOMAS had requested, and THOMAS soon thereafter arrived at the address AUSA Stewart had provided. After the meeting ended, I sent a text message to THOMAS at that number and she responded.

21. During the meeting, THOMAS indicated that the woman who denied knowing her

was “her cousin.” She also said that it was not true that she provided no services to these women.

22. THOMAS acknowledged during this meeting, however, that the billing records that contained her name and described services provided were not accurate or truthful. She said that the entries in those records were written or provided by CRUSE. Each entry on the forms showed to THOMAS stated that THOMAS met with a particular client for 2 hours. Many records included an entry for a 2-hour meeting multiple times in a month. THOMAS denied meeting with her clients for two hours at a time on that many occasions. She said she typically contacted her clients once per month. She said that she did not fill out the forms or submit those billings and that CRUSE was responsible for doing so.

23. THOMAS acknowledged that she did not know Ms. Imes and likely did not provide services to her.

24. THOMAS stated that she was not provided training on how to provide services to her clients or told what to do. She stated that many of her clients told her that they did not need any prenatal care coordination services. As a result, she tried to give them something else they might need by, for example, giving their children fireworks for the Fourth of July.

25. During the interview on November 16, 2022, THOMAS stated that she had communications with CRUSE over Facebook and via text. She thought she may have deleted the text messages, but believed she might still have the Facebook communications on her phone.

26. During the interview on November 16, 2022, THOMAS stated that she had used her phone to video-record a meeting in which CRUSE “did the billing” for the PNCC CTL. She stated that she attended such sessions on a monthly basis during her employment at CTL, which she indicated spanned from June 2021 to sometime in August 2021. THOMAS stated that she filmed this meeting on August 16, 2021 during which CRUSE “did the billing” because she was

not taking notes.¹ She said that CRUSE explained how to fill out the billing sheets. THOMAS told investigators that CRUSE told her not to film it, but that she did anyway. THOMAS showed investigators portions of that video during the interview. During those portions, the screen showed an image of a billing record that included time spent and a description of a service provided. CRUSE could be heard on the video instructing the coordinators not to change the sections that detailed the service provided and to only change the portion of the document that included the care coordinator's name and client's name. THOMAS explained that this was standard – that the billing forms all included essentially the same information for services provided and that CRUSE documented the time spent (almost always 2 hours), and that care coordinators were instructed to only fill in their names and their client names on these billing records.

27. THOMAS also stated that in August 2021, CRUSE paid for her, and other care coordinators, to travel to Las Vegas. THOMAS stated that Ms. Cruse paid for the hotel and flights. THOMAS stated that she had photographs of that trip on her phone.

28. Initially, THOMAS agreed to provide the videos to investigators, but at some point during the meeting, she decided she no longer wanted to speak to law enforcement and ended the interview without providing those videos.

29. Based on the interview with THOMAS's purported clients and THOMAS, it is clear that the billing records used to submit claims for payment to Medicaid by CTL were false.

30. The evidence on THOMAS's phone, particularly the video of CRUSE "doing billing" and teaching care coordinators how to fill out billing records is evidence of health care fraud in violation of 18 U.S.C. 1347.

¹ In an affidavit submitted on November 16, 2022 in support of a warrant to locate THOMAS's phone, the date on which the video was taken was provided as August 6, 2021. This was a typographical error. The correct date, as provided by THOMAS, is August 16, 2021.

31. Investigators from MECEAU reviewed information in the Medicaid Provider Database, kept by DHS in the regular course of its official business, and learned that CTL has had all reimbursement payments directly deposited into an account at US Bank since 03/19/2021. CTL received reimbursements from Wisconsin Medicaid totaling at least \$1,063,022.22.

32. On November 16, 2022, I applied for warrant seeking, among other things, prospective location information for with the cell phone number associated with THOMAS's cell phone. Case agents intend to use the location information, obtained via that warrant, to locate THOMAS's phone in a public place. If and when this warrant issues, case agents will then execute this warrant when THOMAS, with her cell phone, is in a public place.

COMPUTERS, CELLPHONES, ELECTRONIC STORAGE, FORENSIC ANALYSIS

33. As described above and in Attachment B, this application seeks permission to search for evidence that might be found on the person of SAMONE THOMAS in whatever form it may be found. One form in which the records might be found is data stored on a cellphone. Thus, the warrant for which I am applying would authorize the seizure of a cellphone or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

34. *Probable cause.* I submit that if a cellphone is found on the person of THOMAS, there is probable cause to believe records sought by this warrant will be stored on that cellphone, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used

by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

35. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the cellphone recovered from THOMAS’s person because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and

movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

36. *Necessity of seizing or copying entire electronic device.* In most cases, a thorough search of a target location for information that might be stored on electronic storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from a target location, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I am applying would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC UNLOCK

38. The warrant I am applying for would permit law enforcement to obtain from SAMONE THOMAS the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

39. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

40. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the

device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

41. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

42. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

43. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

44. I also know from my training and experience, as well as from information found in

publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

45. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of SAMONE THOMAS to the fingerprint scanner of the device; (2) hold the device in front of the face of SAMONE THOMAS and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

46. I respectfully request a search warrant to be authorized for the search of the person of SAMONE THOMAS, described in Attachment A, to recover and seize evidence described in Attachment B, in any form, including on her Apple iPhone bearing phone number (414) 779-3186.

ATTACHMENT A
Person and Property to Be Searched

1. The person of SAMONE THOMAS (B/F, DOB: XX/XX/1990).
2. THOMAS's Apple iPhone, bearing phone number (414) 779-3186.

ATTACHMENT B
Particular Things to be Seized

1. All records, information, and items related to violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. Section 1320a-7b (Illegal Kickbacks), occurring on or after February 2021, including:

- a. Evidence of communications, photographs, or videos relating to Prenatal Care Coordination client recruitment; care coordinator recruitment; billing; compensation; and/or care coordinator meetings;
- b. Evidence of the performance of care-coordination duties including, but not limited to, communications with clients of Caring Through Love, LLC;
- c. Evidence of communications with individuals for whom Caring Through Love LLC billed for services;
- d. Evidence of communications with care coordinators or owners of care coordinator businesses;
- e. Evidence of compensation or gifts provided by Caring Through Love or Precious Cruse;
- f. Evidence of gifts or items provided to individuals for whom Caring Through Love LLC billed for services
- g. Evidence of travel out of the State of Wisconsin during the period between February 2021 and September 2021;
- h. Evidence of financial transactions related to the provision of care-coordinator services and/or employment with Caring Through Love LLC;
- i. For computers, cellphones, and electronics capable of communication or storage (collectively, “computers”):
 - i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - ii. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - iii. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;

- iv. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- vi. evidence of the times the computer was used;
- vii. passwords, encryption keys, and other access devices that may be necessary to access the computer;
- viii. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- ix. records of or information about Internet Protocol addresses used by the computer;
- x. records of or information about the computer's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- xi. contextual information necessary to understand the evidence described in this attachment;
- xii. lists of contacts and any identifying information.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of SAMONE THOMAS to the fingerprint scanner of the device; (2) hold a device found in front of the face of SAMONE THOMAS and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.